IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH ESDRASCUMEL123@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 24-mj- 250-01-AJ FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Agent Salvatore D. Levatino of the Office of Border Patrol, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Border Patrol Agent - Intelligence ("BPAI") with the United States Department of Homeland Security, Office of Border Patrol ("Border Patrol"). I am currently assigned as an BPAI, and I work at the Beecher Falls Border Patrol Station in Canaan, Vermont.

I have been employed as a Border Patrol Agent since May 2018 and became a BPAI in May 2023. I have completed basic immigration law enforcement training in accordance with 8 CFR § 287.1 by completing basic training at the Federal Law Enforcement Training Center in Artesia, New Mexico from May 2018 to October 2018. I received formal training to identify and investigate alien smuggling and narcotics smuggling activities both at the United States Border Patrol Academy in Artesia, New Mexico from May 2018 to October 2018 and through regular and recurring on-the-job training. In my experience investigating many alien smuggling cases, electronic devices were commonly used to facilitate the smuggling event by arranging the coordination of transportation and by guiding both the smugglers transporting the aliens and the receiving load driver via global positioning system ("GPS") applications and communications relayed over Wi-Fi and/or a telecommunications network.

3. I received training on the use of electronic devices such as computers and mobile phones to further investigative efforts, and I have authored and executed multiple search warrants, to include search warrants on electronic devices.

4. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C). *See* 28 C.F.R. §§ 60.1, 60.2, and 60.3; 8 U.S.C. § 1357, and 8 CFR § 287.5. As a federal law enforcement officer, I am authorized to obtain and execute search warrants issued under the authority of the United States.

5. This affidavit sets forth facts and evidence that are relevant to the requested search warrant but does not set forth all of the facts and evidence that I have gathered during the course of the investigation of this matter. Rather, I have only set forth the facts that are necessary to establish probable cause to support the issuance of the search warrant. This affidavit is based on my own knowledge arising from my participation in this investigation, information provided to

me by other law enforcement officers, and my review of law enforcement reports related to this investigation.

6. The property to be searched is information associated with ESDRASCUMES123@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

7. The applied-for warrant would authorize the release of information associated with ACCOUNT to law enforcement for the purpose of identifying electronically stored data particularly described in Attachment B.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 8 U.S.C. § 1324(a)(1)(A)(ii) (Transportation of an Illegal Alien) and of 8 U.S.C. § 1325 (Illegal Entry) have been committed by Esdras Aaron CALEL-CUMES ("CALEL-CUMES") and Luis Felipe XILOJ-AMBROCIO ("XILOJ-AMBROCIO"), respectively. There is also probable cause to search the property described in Attachment A for evidence of these crimes, further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

9. 8 U.S.C. § 1324(a)(1)(A)(ii), provides, in pertinent part, that that it is unlawful for any person to, knowingly or in reckless disregard of the fact that an alien has come to, entered or

remained in the United States in violation of law, to transport, or move or attempt to transport or move, such alien within the United States by means of transportation or otherwise, in furtherance of such violation of law.

10. 8 U.S.C. § 1325 provides, in pertinent part, that that it is unlawful for any alien [to]…enter[] or attempt[] to enter the United States at any time or place other than as designated by immigration officers, or … elude[] examination or inspection by immigration officers."

PROBABLE CAUSE

11. On September 9, 2024, at approximately 8:25 a.m.., Border Patrol dispatch advised agents of the Beecher Falls Station that a piece of remote surveillance equipment detected and photographed images of one subject walking in the area at 8:24 a.m. This area is remote and undeveloped, located south of the Pittsburg Port of Entry in the northern most part of New Hampshire near the United States/Canada International Border, and in close proximity to US Route 3.

12. Upon receiving the dispatch at 8:25 a.m., agents from the Beecher Falls Border Patrol Station, including Agent Guthrie Peet, reviewed the image and observed what appeared to be one male subject wearing a black and red hat and wearing dark clothing, specifically: black athletic pants with vertical blue stripes, a black hooded sweatshirt with possibly a backpack underneath the sweatshirt, and dirty white sneakers exiting the thick woods and walking towards US Route 3. The images showed the male travelling alone, on foot, and crouching down at times, as if to evade detection.

13. US Route 3 is the only northerly and southerly paved road in the area of the Pittsburg Port of Entry. The location of the remote surveillance equipment is approximately a 30-minute drive from where Agent Peet was located when he received the dispatch at 8:25 a.m.

Upon receiving the dispatch at 8:25 a.m., Agent Peet immediately responded to the area of the remote surveillance equipment by driving northbound on US Route 3.

14. Approximately fifteen minutes into his travel northbound, Agent Peet observed a red Acura RSX bearing Massachusetts registration 4LZJ44 ("Acura") traveling southbound on US Route 3. The Acura was registered to the driver, CALEL-CUMES.[1] It should be noted that Agent Peet did not observe any other vehicles traveling within the five miles approaching the location of the Acura. The location where Agent Peet observed the Acura was consistent in time and location (about halfway) between where he was when he received the dispatch at 8:25 a.m. and where the remote surveillance equipment was located. Additionally, Agent Peet learned via radio communication with the Pittsburg Port of Entry that no vehicles had passed the U.S./Canada Port of Entry at Pittsburg, as the border had only been opened since 8:00 a.m. and no vehicles had crossed in a southerly direction on U.S. Route 3.

15. As the Acura passed Agent Peet's vehicle, Agent Peet observed two adult males seated in the front of the Acura. The individual in the front passenger seat was wearing dark clothing like that of the individual who was captured on image. At this time, Agent Peet turned around to catch back up with the Acura and a vehicle stop was conducted. Agent Peet also called in his location and observations for back-up.

16. Agent Peet identified himself to the two men in the vehicle, who did not respond. Agent Peet asked the two men if they spoke English, to which the driver responded in English, "yes, I understand English." At that point, a female in the backseat who was previously lying down undetected under a blanket removed the blanket and sat up in the vehicle.

17. Agent Peet encountered three people in the vehicle, later identified as follows:

[1] Based on my training and experience, individuals involved in smuggling illegal aliens often utilize vehicles registered from out of state.

- Esdras Aaron CALEL-CUMES, Country of Birth: Guatemala (Driver);
- Luis Felipe XILOJ-AMBROCIO, Country of Birth: Guatemala (Front Passenger); *and*
- Nayelis Carolina MARTINEZ-ARRIAS ("MARTINEZ-ARRIAS"), Country of Birth: Venezuela (Rear Passenger).

18. Agent Peet asked the three individuals in the car if they were U.S. Citizens; and each responded with their country of birth, as described in the previous paragraph.

19. Agent Peet asked if the individuals were present in the United States legally or illegally and CALEL-CUMES shrugged and stated he didn't know if he wanted to answer that. Agent Peet then asked CALEL-CUMES if he had picked up XILOJ-AMBROCIO on the side of the road, and CALEL-CUMES stated that he and MARTINEZ-ARRIAS had driven up to the border and picked up XILOJ-ABROCIO. CALEL-CUMES told Agent Peet that MARTINEZ-ARRIAS was his girlfriend, and they had driven up together. Agent Peet asked CALEL-CUMES if XILOJ-AMBROCIO had crossed into the United States illegally from Canada prior to being picked up, and CALEL-CUMES told Agent Peet that XILOJ-AMBROCIO had crossed the border illegally through the woods, and that they were there to pick him up. Agent Peet asked XILOJ-AMBROCIO in Spanish[2] if he had crossed the border illegally, and he had stated that he had crossed the border through the woods by himself. At this time, Agent Peet collected identification documents from the three passengers. CALEL-CUMES provided Agent Peet with a Massachusetts driver's license, while MARTINEZ-ARRIAS and XILOJ-ABROCIO provided their foreign passports.

[2] Note: Agent Peet is not a fluent Spanish speaker and has limited knowledge of Spanish.

20. During this interaction, Agent Peet noticed that XILOJ-AMBROCIO was wearing a black t-shirt and black shorts but had a red and black hat and a pair of black athletic pants with vertical blue striping sitting on his lap, which was consistent with the clothing that the male in the remote surveillance image. The athletic pants were also covered in dirt, brush, and grass as would be consistent with someone that had just walked through the thick woods.

21. All three subjects were transported to the Beecher Falls Border Patrol Station.

22. At the station, record checks on CALEL-CUMES revealed that he has no legal status in the United Sates. Additionally, record checks on XILOJ-AMBROCIO revealed that he has no legal status in the United States. A record check on MARTINEZ-ARRIAS revealed that she is a citizen of Venezuela who is illegally entered the United States but is awaiting an immigration court date in February of 2025.

23. At approximately 11:07 a.m., Border Patrol Agent Dustin Norsworthy and I conducted an interview of MARTINEZ-ARRIAS. Because MARTINEZ-ARRIAS spoke Spanish, we contacted Adastra, a government provided telephonic interpreter service to request a Spanish interpreter. Interpreter identification # 8399879045 answered our call and assisted by interpreting from English to Spanish and Spanish to English for us. I read MARTINEZ-ARRIAS her *Miranda* rights off of a form in English, which the interpreter translated to her, and she stated that she understood her rights and was willing to speak with us. MARTINEZ-ARRIAS also signed the English *Miranda* waiver form.

24. During this interview, MARTINEZ-ARRIAS stated that she lives in Boston, Massachusetts with her boyfriend, CALEL-CUMES. MARTINEZ-ARRIAS stated she has lived in Boston for eleven months, and currently works at McDonald's. MARTINEZ-ARRIAS stated that earlier that day, she was with her boyfriend, CALEL-CUMES. MARTINEZ-ARRIAS

stated she met CALEL-CUMES online and had an online relationship with him prior to coming to the United States. MARTINEZ-ARRIAS stated she left her house in Boston at 3-3:30 a.m. on September 9, 2024, and got into a vehicle with CALEL-CUMES. MARTINEZ-ARRIAS stated that CALEL-CUMES told her that they were going on a trip, but she didn't know what was happening or where she was going. MARTINEZ-ARRIAS insisted that CALEL-CUMES did not give her any information as to where, when, or how long they were going on a trip, just that she would be back home the night of September 9, 2024, since she had to work the following day.

25. MARTINEZ-ARRIAS stated she they didn't talk about anything during the trip because she was sleeping. MARTINEZ-ARRIAS stated that prior to getting pulled over, they were driving around taking pictures.[3] MARTINEZ-ARRIAS stated that XILOJ-AMBROCIO got into the vehicle, and she was in the back because she was resting. MARTINEZ-ARRIAS did not know XILOJ-AMBROCIO. MARTINEZ-ARRIAS stated that when XILOJ-AMBROCIO entered the car, he said, "good morning," and nothing more.

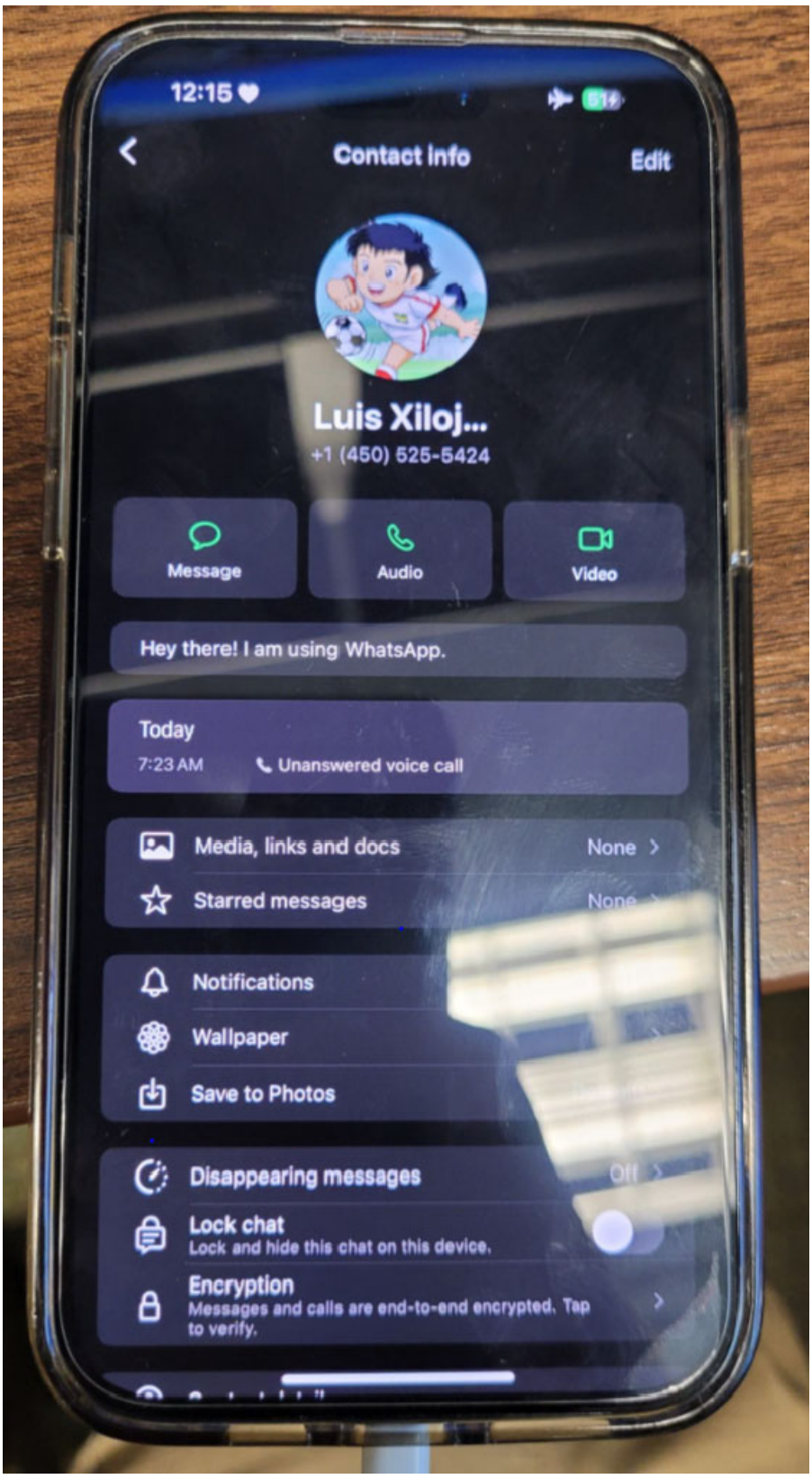
26. MARTINEZ-ARRIAS stated she has no idea why they picked up XILOJ-AMBROCIO, and she had no idea what was going on until she saw the police. MARTINEZ-ARRIAS stated she thought it was odd that they picked up a random person near the border, but it was too late[4] because XILOJ-AMBROCIO had already got in the car. MARTINEZ-ARRIAS stated she did not know XILOJ-AMBROCIO crossed the border illegally. MARTINEZ-ARRIAS stated she was not sure if CALEL-CUMES knew XILOJ-AMBROCIO but guessed he could. MARTINEZ-ARRIAS stated if she knew the answer to why they would pick up a

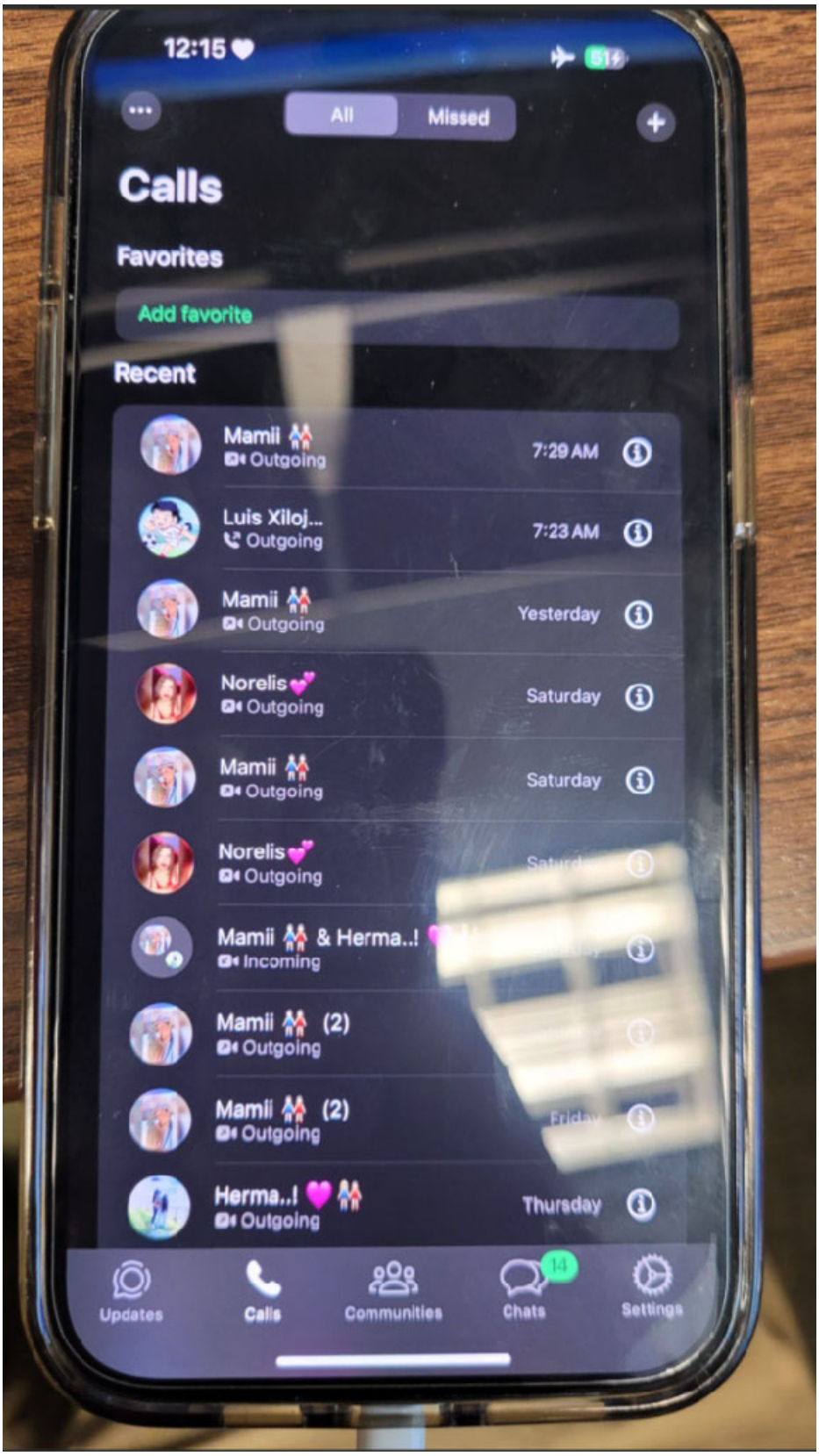
[3] Note: MARTINEZ-ARRIAS did not specify how they were taking pictures (e.g. using a camera or a phone) or what they were taking pictures of.
[4] She did not elaborate on what she meant by "too late."

random person near the border on the side of the road she wouldn't be here. MARTINEZ-ARRIAS stated they were driving for about 4 hours before being pulled over. MARTINEZ-ARRIAS stated when they picked up the XILOJ-AMBROCIO, they did not have to wait for him. MARTINEZ-ARRIAS stated she didn't see if XILOJ-AMBROCIO run out of the woods.

27. MARTINEZ-ARRIAS signed a government provided form consenting to a search her cell phone. This interview was concluded at approximately 11:29 a.m.

28. A cursory search of MARTINEZ-ARRIAS phone revealed a contact in the application "WhatsApp" by the name "Luis Xiloj…" with an unanswered voice call from that contact at 7:23 a.m. I know "WhatsApp" to be an application that allows for video, voice, photo MMS and SMS/text message communication. This missed call was also reflected on the call log for the phone. Photographs of the contact and the call log are below:


12:15
Contact info
Edit
Luis Xiloj...
+1 (450) 525-5424
Message
Audio
Video
Hey there! I am using WhatsApp.
Today
7:23 AM
Unanswered voice call
Media, links and docs
None
Starred messages
None
Notifications
Wallpaper
Save to Photos
Disappearing messages
Off
Lock chat
Lock and hide this chat on this device.
Encryption
Messages and calls are end-to-end encrypted. Tap to verify.


12:15
All
Missed
Calls
Favorites
Add favorite
Recent
Mamii
Outgoing
7:29 AM
Luis Xiloj...
Outgoing
7:23 AM
Mamii
Outgoing
Yesterday
Norelis
Outgoing
Saturday
Mamii
Outgoing
Saturday
Norelis
Outgoing
Mamii & Herma..!
Incoming
Mamii (2)
Outgoing
Mamii (2)
Outgoing
Herma..!
Outgoing
Thursday
Updates
Calls
Communities
Chats
Settings

29. The WhatsApp contact matched the first name and first last name of XILOJ-AMBROCIO. An unanswered phone call from who is suspected of being XILOJ-AMBROCIO to MARTINEZ-ARRIAS is also shown. In my training and experience this appears that this was aids to the suspicion that this was a coordinated smuggling event by all parties involved.

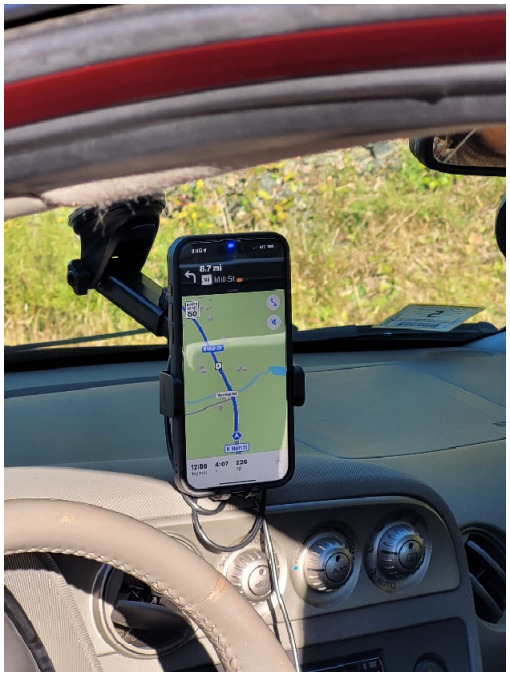
30. After having discovered this information, at approximately 12:25 p.m., Agent Norsworthy and I conducted a second interview of MARTINEZ-ARRIAS. We again contacted Adastra, a government provided telephonic interpreter service to request a Spanish interpreter. Interpreter identification # 37144 answered our call and assisted by interpreting from English to Spanish and Spanish to English for us. This interview was also audio and video recorded.

31. MARTINEZ-ARRIAS stated once again she did not know XILOJ-AMBROCIO. I showed MARTINEZ-ARRIAS the first photo listed at page 10 of this warrant showing XILOJ-AMBROCIO as a contact, and asked her why his number was in her phone if she did not know XILOJ-AMBROCIO. MARTINEZ-ARRIAS stated CALEL-CUMES used her phone that's why XILOJ-AMBROCIO's number was in there. MARTINEZ-ARRIAS stated CALEL-CUMES used the phone because they're a couple. MARTINEZ-ARRIAS stated she was telling me the truth and if she wasn't she wouldn't have given me her phone code. The interview concluded at approximately 12:31 p.m.

32. Based on the foregoing, I believe that there is probable cause to believe that CALEL-CUMES violated 8 U.S.C. § 1324(a)(1)(A)(ii) by transporting or attempting to transport an alien, namely: XILOJ-AMBROCIO, while knowing, or recklessly disregarding that he was an alien who had illegally come to and entered the United States. Additionally, I believe that there is probable cause to believe that XILOJ-AMBROCIO, a national of Guatemala, violated 8 U.S.C. § 1325 by entering the United States at any time or place other than as designated by

immigration officers, and by eluding examination or inspection by immigration officers. Criminal complaints were issued against these Defendants respectively and they both appeared in this Court on Tuesday September 10, 2024 for their initial appearances. Their cases remain pending at this time.

33. Two smartphones were also recovered during the investigation: the first was a black Samsung smartphone in evidence bag # A9932999 recovered off the person of XILOJ-AMBROCIO (hereinafter referred to as the "Samsung Phone") and the second was a black iPhone smartphone in evidence bag # A9932998 recovered off of a phone mount attached to the vehicle's windshield in close proximity to where CALEL-CUMES was seated as the driver of the vehicle (hereinafter referred to as the "iPhone"). A photograph of this particular iPhone as it appeared in the vehicle prior to seizure is attached below:



34. On Monday, September 16, 2024, a search warrant for the Samsung Phone and the iPhone was authorized by this Court, the Honorable Andrea K. Johnstone on docket 24-mj-238-01-AJ.

35. On Tuesday, September 17, 2024, I delivered the Samsung Phone and the iPhone to the U.S. Border Patrol Swanton Sector Intelligence Unit to conduct a forensic examination and extraction of the two devices. While the Samsung Phone was able to be downloaded, the iPhone attributed to CALEL-CUMES was protected by a six-digit passcode and therefore could not be fully downloaded. It was also running on a relatively new operating system that was not supported by the forensic software utilized by our Digital Forensic analysts to bypass passcodes, including Cellebrite Premium and GrayKey. A Before First Unlock (BFU) partial extraction was able to be performed on the iPhone, however this information does not provide a complete picture of the communications on the device. A BFU partial extraction will include limited user data, including voicemails, partial multimedia, system metadata, partial application data and account data. The BFU extraction lacked third party applications and messaging data.

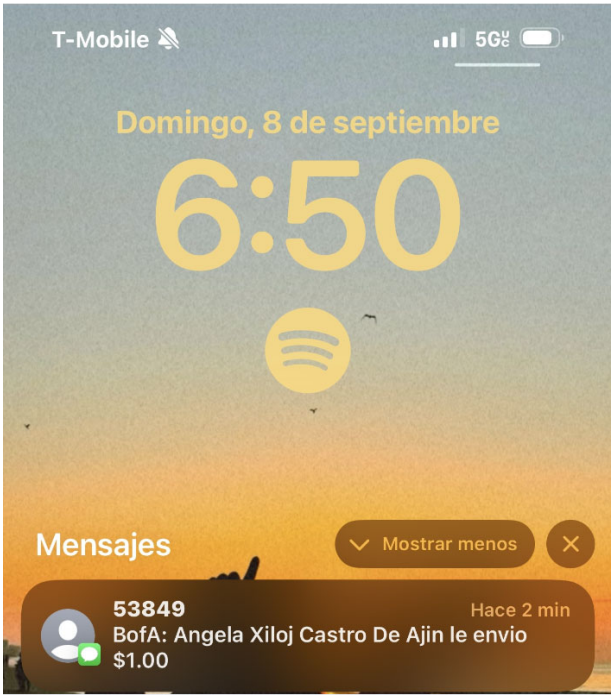
36. Analysts were able to observe from the BFU extraction of the iPhone that the iPhone had uploaded to Apple's iCloud on 9/8/2024 at 11:26 PM[5] EST and was associated with the Apple ID: ESDRASCUMES123@gmail.com. Therefore, by virtue of having an Apple ID, there is also an iCloud associated with the Apple account ESDRASCUMES123@gmail.com.

37. While searching the Samsung Phone, it appears XILOJ-AMBROCIO was messaging 774-486-8809 with the associated contact name saved as "Aaron". It should be noted that "Aaron" is the middle name of CALEL-CUMES. 774-486-8809 is one of two phone numbers associated to CALEL-CUMES's iPhone, according to the information received in the BFU partial extraction. Based on my observations of communications between the Samsung Phone and 774-486-8809, I believe that, at a minimum, evidence in the form of the same communications may be observed on the Apple iCloud upload.

[5] Note: the times provided in the extraction were in UTC +0, so I have converted the times in this affidavit to reflect EST for purposes of this affidavit.

38. In reviewing the data on from the Samsung Phone, I utilized Google Translate Spanish Language to English Language, given that I do not speak Spanish at a level of a native speaker. Although not a direct translation, it appears in my training and experience that the messages between the Samsung Phone and 774-486-8809 show discussions of where to send payment via Zelle and CALEL-CUMES asking XILOJ-AMBROCIO for his real time location which, based on my training and experience, is a tactic commonly used by smugglers to pick up illegal aliens to further their illegal entry.

39. Additionally, the Samsung Phone contained a screenshot, dated September 8, 2024, at 6:54 P.M. appearing to show an Angela XILOJ CASTRO DE AJIN sending CALEL-CUMES $1.



40. According to the data extracted from the Samsung Phone, it appears that XILOJ-AMBROCIO was also messaging 774-486-0937, with the associated contact name saved as "Aron 2". This number was identified as MARTINEZ-ARRIAS phone number via the consent

search of her phone. MARTINEZ-ARRIAS stated in her interview CALEL-CUMES was utilizing her phone before the smuggling event.

41. On September 9, 2024, at 4:58 A.M. XILOJ-AMBROCIO received a call from 774-468-8809 that was answered and lasted 6 minutes and 6 seconds. Another phone call to 774-468-8809 from XILOJ-AMBROCIO was attempted at 5:09 A.M. but not answered. XILOJ-AMBROCIO attempted to call 774-468-8809 again at 5:07 A.M. but it was not answered. XILOJ AMBROCIO had a missed call from 774-468-8809 at 7:22 A.M.

42. On September 9, 2024, at 5:04 A.M. XILOJ-AMBROCIO received a call from 774-486-0937, the number associated with MARTINEZ-ARRIAS' phone, that was answered and lasted 43 seconds.

43. I submitted a preservation request to Apple for the Apple ID ESDRASCUMES123@gmail.com on September 25, 2024, and Apple confirmed receipt of the preservation request on September 26, 2024 with a reference ID of 202400810290.

44. Based on my training, experience, and familiarity with the context of this investigation, I know that the Apple ID ESDRASCUMES123@gmail.com is likely to contain some or all of the records and information described with particularity in Attachment B, in part because the direct action activity described above would require coordination and planning that Cellbrite and GrayKey were not able to download, and it appears from a review of the Samsung Phone that XILOJ-AMBROCIO was communicating with 774-486-8809, which is associated with the physical device of the iPhone and may be uploaded in part or in whole to the Apple iCloud.

BACKGROUND CONCERNING APPLE[6]

45. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

46. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and

[6] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be

purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

47. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

48. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

49. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

50. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

51. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

52. In this case, there was a coordinated pick-up of an illegal alien who illegally entered the United States through a densely forested and remote area of the U.S. / Canadian border. This crime required planning, and according to at least one witness statement, CALEL-CUMES was in communication with XILOJ-AMBROCIO via messaging applications. Where there is evidence to suggest that the Samsung Phone was in communication with a phone number associated with the iPhone, and that the iPhone was also observed unlocked and showing a map with directions to a location, this messaging and navigation information could be used to uncover potential secondary locations for alien smuggling and/or other co-conspirators involved in the transportation of illegal aliens in violation of 8 U.S.C. § 1324(a)(1)(A)(ii) (Transportation of an Illegal Alien) and of 8 U.S.C. § 1325 (Illegal Entry). Therefore, in my training and experience,

evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

53. Cellebrite could not access the data associated with all applications and messaging system on the iPhone, given that only a BFU partial extraction was able to be completed without the iPhone's passcode. From the interview with MARTINEZ-ARRIAS indicating that CALEL-CUMES used her phone to contact XILOJ-AMBROCIO, coupled with the evidence from the Samsung Phone showing that the Samsung Phone was in communication with a phone number associated with the iPhone, and that this iPhone was backed up to the Cloud the night before the illegal border crossing and subsequent illegal transportation, it is believed that CALEL-CUMES was utilizing his iPhone to coordinate this smuggling event, and that the Apple iCloud may contain evidence of this illegal smuggling event. Therefore, the Apple iCloud data may contain data from any data not captured by the BFU partial extraction to show who CALEL-CUMES was communicating with in different formats, to wit: photo, video, voice, text and other formats. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

54. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account

may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

55. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store, such as Telegram, Signal, Proton Mail, Proton VPN, Messenger, Sidechat, WhatsApp, and Snapchat, may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators in the alien smuggling operation. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

56. Therefore, Apple's servers are likely to contain stored electronic communications that have heretofore been unable to be viewed by law enforcement and contain information and evidence about the planning, coordination, and execution of 8 U.S.C. § 1324(a)(1)(A)(ii) (Transportation of an Illegal Alien) and of 8 U.S.C. § 1325 (Illegal Entry). This information may also be used to identify CALEL-CUMES' and XILOJ-AMBROCIO's co-conspirators.

CONCLUSION

57. Based on the forgoing, I request that the Court issue the proposed search warrant.

58. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then

compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Salvatore D. Levatino
Salvatore D. Levatino
Border Patrol Agent – Intelligence
United States Border Patrol

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Sep 30, 2024**
Time: **9:36 AM, Sep 30, 2024**

Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with ESDRASCUMES123@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data including but not limited to communication contents in applications, as well as all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within seven (7) days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 8 U.S.C. § 1324(a)(1)(A)(ii) (Transportation of an Illegal Alien) and of 8 U.S.C. § 1325 (Illegal Entry) involving CALEL-CUMES and XILOJ-AMBROCIO occurring in the time leading up to September 9, 2024, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The Transportation of an Illegal Alien and Illegal Entry of XILOJ-AMBROCIO on/about September 9, 2024, in Pittsburg, New Hampshire, or other locations associated with the U.S. – Canadian border;

b. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

c. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the U.S. Border Patrol may deliver a

complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature